

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur : L'ADMINISTRATION CHARGÉE DE
L'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Destinataire :

KOHR, Martin
THOMSON
46, Quai A. Le Gallo
F-92648 Boulogne Cedex
FRANCE



PCT

CL

NOTIFICATION DE TRANSMISSION DU
RAPPORT PRÉLIMINAIRE
INTERNATIONAL SUR LA BREVETABILITÉ
(règle 71.1 du PCT)

Date d'expédition
(jour/mois/année)

24.02.2005

Référence du dossier du déposant ou du mandataire
PF030167

NOTIFICATION IMPORTANTE

Demande internationale No.
PCT/FR 03/03250

Date du dépôt international (jour/mois/année)
30.10.2003

Date de priorité (jour/mois/année)
30.10.2002

Déposant
THOMSON LICENSING S.A. et al.

- Il est notifié au déposant que l'administration chargée de l'examen préliminaire international a établi le rapport préliminaire international sur la brevetabilité pour la demande internationale et le lui transmet ci-joint, accompagné, le cas échéant, de ces annexes.
- Une copie du présent rapport et, le cas échéant, de ses annexes est transmise au Bureau international pour communication à tous les offices élus.
- Si tel ou tel office élu l'exige, le Bureau international établira une traduction en langue anglaise du rapport (à l'exclusion des annexes de celui-ci) et la transmettra aux offices intéressés.

4. NOTIFICATION IMPORTANTE

Pour aborder la phase nationale auprès de chaque office élu, le déposant doit accomplir certains actes (dépôt de traduction et paiement des taxes nationales) dans le délai de 30 mois à compter de la date de priorité (ou plus tard pour ce qui concerne certains offices) (article 39.1) (voir aussi le rappel envoyé par le Bureau international dans le formulaire PCT/IB/301).

Lorsqu'une traduction de la demande internationale doit être remise à un office élu, elle doit comporter la traduction de toute annexe du rapport préliminaire international sur la brevetabilité. Il appartient au déposant d'établir la traduction en question et de la remettre directement à chaque office élu intéressé.

Pour plus de précisions en ce qui concerne les délais applicables et les exigences des offices élus, voir le Volume II du Guide du déposant du PCT.

Il est signalé au déposant que l'article 33(5) stipule que les critères de nouveauté, d'activité inventive et d'application industrielle tels que définis à l'article 33(2) à (4) ne servent qu'aux fins de l'examen préliminaire international et que "tout État contractant peut appliquer des critères additionnels ou différents afin de décider si, dans cet État, l'invention est brevetable ou non" (voir également l'article 27(5)). De tels critères additionnels peuvent par exemple avoir rapport à des exceptions à la brevetabilité ainsi qu'à des exigences concernant l'exposé suffisant de l'invention, la clarté des revendications et leur fondement sur la description.

Nom et adresse postale de l'administration chargée de l'examen
préliminaire international



Office européen des brevets - P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tél. +31 70 340 - 2040 Tx: 31 651 epo nl
Fax: +31 70 340 - 3016

Fonctionnaire autorisé

Bergström, C



Tel. +31 70 340-2898



TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

PCT

RAPPORT PRÉLIMINAIRE INTERNATIONAL SUR LA BREVETABILITÉ (chapitre II du Traité de coopération en matière de brevets)

Référence du dossier du déposant ou du mandataire	POUR SUITE À DONNER voir formulaire PCT/PEA/416	
Demande internationale No. PCT/FR 03/03250	Date du dépôt international (jour/mois/année) 30.10.2003	Date de priorité (jour/mois/année) 30.10.2002
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L29/06		
Déposant THOMSON LICENSING S.A. et al.		
<p>1. Le présent rapport est le rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international en vertu de l'article 35 et transmis au déposant conformément à l'article 36.</p> <p>2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.</p> <p>3. Ce rapport est accompagné d'ANNEXES, qui comprennent :</p> <p>a. <input type="checkbox"/> un total de (envoyées au déposant et au Bureau international) feuilles, définies comme suit :</p> <p><input type="checkbox"/> les feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou des feuilles contenant des rectifications autorisées par la présente administration (voir la règle 70.16 et l'instruction administrative 607).</p> <p><input type="checkbox"/> des feuilles qui remplacent des feuilles précédentes, mais dont la présente administration considère qu'elles contiennent une modification qui va au-delà de l'exposé de l'invention qui figure dans la demande internationale telle qu'elle a été déposée, comme il est indiqué au point 4 du cadre n° I et dans le cadre supplémentaire.</p> <p>b. <input type="checkbox"/> (envoyées au Bureau international seulement) un total de (préciser le type et le nombre de support(s) électronique(s)) , qui contiennent un listage de la ou des séquences ou un ou des tableaux y relatifs, déposés sous forme déchiffrable par ordinateur seulement, comme il est indiqué dans le cadre supplémentaire relatif au listage de la ou des séquences (voir l'instruction administrative 802).</p>		
<p>4. Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants :</p> <p><input checked="" type="checkbox"/> Cadre n° I Base de l'opinion</p> <p><input type="checkbox"/> Cadre n° II Priorité</p> <p><input type="checkbox"/> Cadre n° III Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle</p> <p><input type="checkbox"/> Cadre n° IV Absence d'unité de l'invention</p> <p><input checked="" type="checkbox"/> Cadre n° V Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration</p> <p><input type="checkbox"/> Cadre n° VI Certains documents cités</p> <p><input type="checkbox"/> Cadre n° VII Irrégularités dans la demande internationale</p> <p><input type="checkbox"/> Cadre n° VIII Observations relatives à la demande internationale</p>		
Date de présentation de la demande d'examen préliminaire internationale 06.05.2004	Date d'achèvement du présent rapport 24.02.2005	
Nom et adresse postale de l'administration chargée de l'examen préliminaire international  Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Fonctionnaire autorisé Olachea, F N° de téléphone +31 70 340-4352 	

Demande internationale n°
PCT/FR 03/03250

BEST AVAILABLE COPY

**RAPPORT PRÉLIMINAIRE INTERNATIONAL
SUR LA BREVETABILITÉ**

Demande internationale n°
PCT/FR 03/03250

Cadre n° V Déclaration motivée selon l'article 35.2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

- | | | | |
|--|------|----------------|-----|
| 1. Déclaration | | | |
| Nouveauté | Oui: | Revendications | 1-4 |
| | Non: | Revendications | |
| Activité inventive | Oui: | Revendications | 1-4 |
| | Non: | Revendications | |
| Possibilité d'application industrielle | Oui: | Revendications | 1-4 |
| | Non: | Revendications | |

2. Citations et explications (règle 70.7) :

voir feuille séparée

**RAPPORT PRÉLIMINAIRE INTERNATIONAL
SUR LA BREVETABILITÉ
(FEUILLE SEPARÉE)**

Demande internationale n°

PCT/FR 03/03250

Concernant le point V

Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1 Il est fait référence au document suivant:

D1: MENEZES ET AL: "Handbook of Applied Cryptography, PASSAGE"
HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON
DISCRETE MATHEMATICS AND ITS APPLICATIONS, BOCA RATON,
FL, CRC PRESS, US, 1997, pages 497-552, XP002248262 ISBN: 0-8493-
8523-7

2 Le document D1, qui est considéré comme étant l'état de la technique le plus proche de l'objet de la revendication 1, décrit (les références entre parenthèses s'appliquent à ce document) :

Procédé de renouvellement de clé symétrique dans un réseau de communication comprenant un dispositif d'un premier type contenant:

- une première clé symétrique pour chiffrer des données à transmettre à un dispositif d'un second type raccordé au réseau; (passage 12.3.1.i) et
- ladite première clé symétrique chiffrée avec une seconde clé symétrique de réseau connue d'au moins un dispositif d'un second type raccordé audit réseau (passage 12.3.1.i);

le procédé comportant les étapes qui consistent, pour le dispositif d'un premier type, à:

- a - générer un nombre aléatoire (passage 12.19.ii, "Point to point key update by key derivation and non-reversible functions");
- b - calculer une nouvelle clé symétrique fonction de la seconde clé symétrique de réseau et dudit nombre aléatoire (passage 12.19.ii, "Point to point key update by key derivation and non-reversible functions");
- c - chiffrer les données à transmettre avec la nouvelle clé symétrique (passage 12.19.ii, "Point to point key update by key derivation and non-reversible functions"); et

- d - transmettre à un dispositif d'un second type, via ledit réseau:
- les données chiffrées avec la nouvelle clé symétrique;
 - le nombre aléatoire; et
 - ladite première clé symétrique chiffrée avec la seconde clé symétrique de réseau (passage 12.19.ii, "Point to point key update by key derivation and non-reversible functions").

Par conséquent, l'objet de la revendication 1 diffère de D1 en ce que la clé de réseau est connue **uniquement** par les dispositifs d'un second type (donc n'étant pas partagée par les deux dispositifs) et que la nouvelle clé symétrique est calculée à partir de la première clé symétrique et d'un nombre aléatoire.

L'objet de la revendication 1 est donc nouveau (article 33(2) PCT).

Le problème que la présente invention se propose de résoudre est comment améliorer la sécurité de renouvellement de clé.

- 2.1 Les revendications 2-4 dépendent de la revendication 1 satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.